修士論文の和文要旨

大学院　電気通信学　研究科　　博士前期課程		情報工学　専攻
氏　　名	渡部 信吾	学籍番号　　0531036
論　文　題　目	FPGA による真の乱数の生成	

要　　旨

モンテカルロ法などのシミュレーション分野や，暗号およびセキュリティ分野における鍵生成，鍵交換，回路のマスクなどでは，大量の乱数やよく散らばった(乱数性の良い) 乱数が必要とされることが多い．乱数には大きく分けて真の乱数と疑似乱数がある．真の乱数とは予測が不可能で再現性のない乱数のことである．通常は熱雑音や核分裂等の本質的にランダムな物理的事象を元に乱数を生成し，離散化・符号化の後に後処理をする．アナログ回路を必要とするので外部回路を付加することが多い．一方，プログラマブルなデジタル回路である FPGA (Field Programmable Gate Array) を用い外部回路を要しない真の乱数の生成手法が提案されている．FPGA の内部で閉じた回路が構成できるので，耐タンパー性，コストの削減，IP コアとしての回路などの面で有用である．

FPGA の資源はルックアップテーブルやレジスタを含む論理素子と配線資源 (Interconnect) とからなる．本研究では FPGA のみで構成される真の乱数生成器に着目し，まず，リングオシレータの長さが乱数性に及ぼす影響を実験的に調べた．次にリングオシレータを構成する NOT ゲートを FPGA の配線資源で置き換えた時のリングオシレータの乱数性を実験的に調べた．その結果，極端に短いリングオシレータでは乱数性が低く，NOT ゲートより配線資源の方が遅延に対するジッターの割合が大きいことがわかった．従って，ある程度長い遅延のリングオシレータを Interconnect を用いて作成することにより，乱数性の向上と論理回路資源の節約の双方が達成できると期待される．